Employee Post-Travel Disclosure of Travel Expenses

Date/Time Stamp:

SECRETARY OF THE SENATE
17 SEP -8 PM 2:32

Post-Travel Filing Instructions: Complete this form within **30 days** of returning from travel. Submit all forms to the **Office of Public Records in 232 Hart Building.**

In compliance with Rule 35.2(a) and (c), I make the following disclosures with respect to travel expenses that have been or will be reimbursed/paid for me. I also certify that I have attached:

☐ The **original** *Employee Pre-Travel Authorization* (Form RE-1), **AND**
☐ A **copy** of the *Private Sponsor Travel Certification Form* with all attachments (itinerary, invitee list, etc.)

Private Sponsor(s) (list all): Stanford University's Hoover Institution

Travel date(s): _____

Name of accompanying family member (if any): N/A
Relationship to Traveler: ☐ Spouse ☐ Child

IF THE COST OF LODGING **DID NOT INCREASE** DUE TO THE ACCOMPANYING SPOUSE OR DEPENDENT CHILD, ONLY INCLUDE LODGING COSTS IN EMPLOYEE EXPENSES. (Attach additional pages if necessary.)

Expenses for Employee:

	Transportation Expenses	**Lodging Expenses**	**Meal Expenses**	**Other Expenses (Amount & Description)**
☐ Good Faith Estimate ☒ Actual Amount	$579.29 - Flight	$450	$182.50	$82.63 - Ground Transportation

Expenses for Accompanying Spouse or Dependent Child (if applicable):

	Transportation Expenses	**Lodging Expenses**	**Meal Expenses**	**Other Expenses (Amount & Description)**
☐ Good Faith Estimate ☐ Actual Amount	N/A	N/A	N/A	N/A

Provide a description of all meetings and events attended. *See* Senate Rule 35.2(c)(6). (Attach additional pages if necessary.):

See Attached Syllabus

9.8.17 — Michael Stransky — Michael Stransky
(Date) *(Printed name of traveler)* *(Signature of traveler)*

TO BE COMPLETED BY SUPERVISING MEMBER/OFFICER:

I have made a determination that the expenses set out above in connections with travel described in the *Employee Pre-Travel Authorization* form, are necessary transportation, lodging, and related expenses as defined in Rule 35.

9/8/17 — John Barrasso
(Date) *(Signature of Supervising Senator/Officer)*

(Revised 1/3/11)

Form RE-2

0000000057564

Date/Time Stamp:

EMPLOYEE PRE-TRAVEL AUTHORIZATION

Pre-Travel Filing Instructions: Complete and submit this form at least 30 days prior to the travel departure date to the **Select Committee on Ethics** in **SH-220**. Incomplete and late travel submissions will **not** be considered or approved. This form **must** be typed and is available as a fillable PDF on the Committee's website at ethics.senate.gov. Retain a copy of your entire pre-travel submission for your required post-travel disclosure.

ETHIC JUL13'17PM 3:45

Name of Traveler: Michael K. Stransky

Employing Office/Committee: Senate Republican Policy Committee

Private Sponsor(s) (list all): Stanford University Hoover Institution

Travel date(s): August 14-17, 2017

*Note: If you plan to extend the trip for any reason you **must** notify the Committee.*

Destination(s): Palo Alto, CA (Stanford University)

Explain how this trip is specifically connected to the traveler's official or representational duties:

I cover cybersecurity and national security issues for a Senate leadership office. Travel is to an educational seminar examining cybersecurity issues for legislative staff. Participation in this seminar will directly provide increased substantive knowledge on a topic at the core of my issue portfolio, and introduce me to other staff and academic practitioners working in the field on these issues, making them available to me in the future as a resource in my work.

Name of accompanying family member (if any): _____

Relationship to Employee: ☐ Spouse ☐ Child

I certify that the information contained in this form is true, complete and correct to the best of my knowledge:

7/13/17
(Date)

(Signature of Employee)

TO BE COMPLETED BY SUPERVISING SENATOR/OFFICER (President of the Senate, Secretary of the Senate, Sergeant at Arms, Secretary for the Majority, Secretary for the Minority, and Chaplain):

I, John Barrasso hereby authorize Michael Stransky
(Print Senator's/Officer's Name) *(Print Traveler's Name)*

an employee under my direct supervision, to accept payment or reimbursement for necessary transportation, lodging, and related expenses for travel to the event described above. I have determined that this travel is in connection with his or her duties as a Senate employee or an officeholder, and will not create the appearance that he or she is using public office for private gain.

I have also determined that the attendance of the employee's spouse or child is appropriate to assist in the representation of the Senate. *(signify "yes" by checking box)* ☐

7/13/17
(Date)

(Signature of Supervising Senator/Officer)

0000000057365

(Revised 10/19/15)

Form RE-1

Stanford University

Dear Congressional Staff,

On behalf of Hoover Institution fellows Mike Franc, Herb Lin and Amy Zegart, I would like to formally invite you to participate in Stanford's Congressional Cyber Boot Camp, held in Palo Alto, California on **August 14th – 17th, 2017.** The boot camp is a cross-institutional program created by Stanford's Hoover Institution, Center for International Security and Cooperation, and Freeman Spogli Institute for International Studies.

Designed to give select senior congressional staffers a deeper understanding of cybersecurity issues, the boot camp incorporates a broader network of experts from industry and academia to draw upon in the future. You will examine key technical, legal, economic, psychological, and organizational cyber policy challenges, participate in hands on simulations, taught by world renowned faculty, and engage in discussions with Silicon Valley leaders. We have also dedicated time for dialogue and questions that are of particular interest to you.

Confirmed speakers this year include: former Secretary of State Condoleezza Rice, former Ambassador to Russia Michael McFaul, former President of Estonia Toomas Hendrik Ilves, co-founder of Andreessen Horowitz, Marc Andreessen, plus many more from academia, tech, and the policy community. A field trip to Tesla's factory and headquarters is also slated on the agenda.

Stanford University will pay for reasonable travel expenses, including round-trip economy airfare, and ground transportation, business class lodging, and meals. The Boot Camp will not be financed in any part by a registered lobbyist or foreign agent, and will comply with all Congressional ethics rules. ***To participate in the Congressional Cyber Boot Camp, please reply to Andrew Clark, afclark@stanford.edu, no later than June 30th.***

We are very much looking forward to your participation and welcoming you to sunny California this August.

Sincere regards,

Russell C. Wald
Senior Manager for External Affairs
Hoover Institution, Stanford University

HOOVER INSTITUTION
Ideas Defining A Free Society

Cyber Boot Camp 2017
Stanford University
Palo Alto, CA

Group Flight Information:

Outbound flight: August 14, 2017
Flight Number – VX 67
Departure Airport – IAD
Departure Time – 7:20am
Arrival Airport – SFO
Arrival Time – 9:55am

Return Flight: August 17, 2017
Flight Number – VX 1
Departure Airport – SFO
Departure Time – 8:00am
Arrival Airport – DCA
Arrival Time – 4:05pm

0000000057 87

Last Name	First Name	Title	Committee/Office	Chamber	Party	Gender
Akpa	Stephanie	Policy Counsel	Senator Warren	Senate	D	F
Arias	Jonathan	MLA	Senator Rubio	Senate	R	M
Batch	Brandon	Senior LA	Rep. McCaul	House	R	M
Bergin	Moira	Staff Director	Homeland Subcommittee	House	D	F
Bergreen	Tim	Democratic Staff Director	HPSCI	House	D	M
Burchfield	James	PSM	Committee on Small Business	House	R	M
Burwell	Carter	Deputy Chief Counsel	Subcommittee on Constitution (Judiciary)	Senate	R	M
Carroll	Melika	Policy Advisor	Senator Schatz	Senate	D	F
Dressler	Jeff	National Security Advisor	Speaker Ryan	House	R	M
Everett	Jason	Chief Counsel	Judiciary Sub	House	D	M
Freedman	Brett	Counsel	SSCI	Senate	D	M
Geer	Harlan	National Security Advisor	Senator Hassan	Senate	D	M
Hiller	Aaron	Chief Oversight Counsel	Committee on Judiciary	House	D	M
Jacobson	Corey	Senior Policy Advisor	Rep. Ted Lieu	House	D	M
Keeley	Joe	Chief Counsel	Judiciary Sub (Courts, IP, Internet)	House	R	M
Khrestin	Igor	National Security Advisor	Senator Garner	Senate	R	M
King	Elizabeth	Staff Director	SASC	Senate	D	F
Kitchen	Klon	National Security Advisor	Sasse	Senate	R	M
Klein	Julie	PSM	HSGAC	Senate	D	F
Lazarus	Allison	PSM	SASC	Senate	R	F
Lips	Dan	PSM	HSGAC	Senate	R	M
Lipsky	Kim	Democratic Staff Director	Commerce, Science, Transportation	Senate	D	F
Lynch	Tim	Senior Counsel	Oversight and Gov Reform	House	D	M
Matthews	Madeline	PSM	Subcommittee on Cyber (Homeland)	House	R	F
McElivein	Elizabeth	PSM	Judiciary Committee	House	D	F
McFeely	Tara	PSM	SSCI	Senate	R	F

Middleton	Bakari	Counsel	Booker	Senate	D	M
Nguyen	Minh	General Counsel	Senator McCain	Senate	R	F
Park	Chan	General Counsel	Committee on Judiciary	Senate	D	M
Po	Rosa	Deputy Chief of Staff	Senator Klobuchar	Senate	D	F
Ravindra	Arjun	PSM	SSCI	Senate	R	M
Rossi	Nick	Staff Director	Commerce, Science, Transportation	Senate	R	M
Smith	Angel	PSM	HPSCI	House	R	F
Soifer	Halie	National Security Advisor	Senator Harris	Senate	D	F
Steward	Lindsay	PSM	Subcommittee Oversight	House	R	F
Stock	Troy	Senior Counsel	Oversight	House	R	M
Tuttle	Chris	Staff Director	Foreign Relations	Senate	R	M

PRIVATE SPONSOR TRAVEL CERTIFICATION FORM

This form must be completed by any private entity offering to provide travel or reimbursement for travel to Senate Members, officers, or employees (Senate Rule 35, clause 2). Each sponsor of a fact-finding trip must sign the completed form. The trip sponsor(s) must provide a copy of the completed form to each invited Senate traveler, who will then forward it to the Ethics Committee with any other required materials. The trip sponsor(s) should **NOT** submit the form directly to the Ethics Committee. Please consult the accompanying instructions for more detailed definitions and other key information.

The Senate Member, officer, or employee **MUST** also provide a copy of this form, along with the appropriate travel authorization and reimbursement form, to the Office of Public Records (OPR), Room 232 of the Hart Building, within thirty (30) days after the travel is completed.

---

1. Sponsor(s) of the trip (please list all sponsors): Stanford University's Hoover Institution

2. Description of the trip: An intensive program for congressional staff which consists of three days of seminars, simulations, and keynote presentations.

3. Dates of travel: 08/14/2017 - 08/17/2017

4. Place of travel: Stanford University, Palo Alto, CA

5. Name and title of Senate invitees: See attached list

6. I *certify* that the trip fits one of the following categories:

☐ (A) The sponsor(s) are not registered lobbyists or agents of a foreign principal **and** do not retain or employ registered lobbyists or agents of a foreign principal **and** no lobbyist or agents of a foreign principal will accompany the Member, officer, or employee *at any point* throughout the trip.

– OR –

☒ (B) The sponsor or sponsors are not registered lobbyists or agents of a foreign principal, but retain or employ one or more registered lobbyists or agents of a foreign principal and the trip meets the requirements of Senate Rule 35.2(a)(2)(A)(i) or (ii) *(see question 9)*.

7. ☒ I *certify* that the trip will not be financed in any part by a registered lobbyist or agent of a foreign principal.

– AND –

☒ I *certify* that the sponsor or sponsors will not accept funds or in-kind contributions earmarked directly or indirectly for the purpose of financing this specific trip from a registered lobbyist or agent of a foreign principal or from a private entity that retains or employs one or more registered lobbyists or agents of a foreign principal.

8. I *certify* that:

☒ The trip will not in any part be planned, organized, requested, or arranged by a registered lobbyist or agent of a foreign principal except for *de minimis* lobbyist involvement.

– AND –

☒ The traveler will not be accompanied on the trip by a registered lobbyist or agent of a foreign principal except as provided for by Committee regulations relating to lobbyist accompaniment (*see question 9*).

9. **USE ONLY IF YOU CHECKED QUESTION 6(B)**
I *certify* that if the sponsor or sponsors retain or employ one or more registered lobbyists or agents of a foreign principal, one of the following scenarios applies:

☐ (A) The trip is for attendance or participation in a one-day event (exclusive of travel time and one overnight stay) and no registered lobbyists or agents of a foreign principal will accompany the Member, officer, or employee *on any segment* of the trip.

– OR –

☐ (B) The trip is for attendance or participation in a one-day event (exclusive of travel time and two overnight stays) and no registered lobbyists or agents of a foreign principal will accompany the Member, officer, or employee *on any segment* of the trip (*see questions 6 and 10).*

– OR –

☒ (C) The trip is being sponsored only by an organization or organizations designated under § 501(c)(3) of the Internal Revenue Code of 1986 and no registered lobbyists or agents of a foreign principal will accompany the Member, officer, or employee *at any point* throughout the trip.

10. **USE ONLY IF YOU CHECKED QUESTION 9(B)**
If the trip includes two overnight stays, please explain why the second night is practically required for Senate invitees to participate in the travel:

11. ☒ An itinerary for the trip is attached to this form. I *certify* that the attached itinerary is a detailed (hour-by-hour), complete, and final itinerary for the trip.

12. Briefly describe the role of each sponsor in organizing and conducting the trip:

Stanford University's Hoover Institution solely planned all aspects of the trip, including topics to be discussed, travel/accommodation logistics, and required paperwork. Hoover employees will also be responsible for traveling with congressional staff and managing logistics for the duration of the trip.

13. Briefly describe the stated mission of each sponsor and how the purpose of the trip relates to that mission:

The Hoover Institution is a research institution that seeks to improve the human condition by advancing ideas that promote economic opportunity and prosperity while securing and safeguarding the peace through its world renowned scholars, library, and archives, as well as by engaging Congress and its staff.

14. Briefly describe each sponsor's prior history of sponsoring congressional trips:

This is the third sponsored trip for congressional staff organized by the Hoover Institution. The latest of which was in April of 2017 and had a similar format as this trip.

15. Briefly describe the educational activities performed by each sponsor (other than sponsoring congressional trips):

Stanford University's Hoover Institution regularly sponsors policy panels and roundtables for think tank scholars, journalists, congressional staff, Executive branch officials, academics, and members of the general public.

16. Total Expenses for Each Participant:

	Transportation Expenses	Lodging Expenses	Meal Expenses	Other Expenses
☒ Good Faith estimate ☐ Actual Amounts	$600 roundtrip airfare; $200 ground transportation	$450 total ($150/night)	$192 total ($64/day)	N/A

17. State whether a) the trip involves an event that is arranged or organized *without regard* to congressional participation or b) the trip involves an event that is arranged or organized *specifically with regard* to congressional participation:

The trip is arranged/organized specifically for congressional participation.

18. Reason for selecting the location of the event or trip

In order to have a significant number of Hoover senior fellows participate in the event, we are hosting at the Hoover Institution's headquarters on the Stanford University campus.

19. Name and location of hotel or other lodging facility:

Schwab Residential Center, 680 Serra St., Stanford, CA 94305

20. Reason(s) for selecting hotel or other lodging facility:

Schwab Residential Center is owned and operated by Stanford. It is in close proximity to the events that comprise the program.

21. Describe how the daily expenses for lodging, meals, and other expenses provided to trip participants compares to the maximum per diem rates for official Federal Government travel:

All lodging, meals, and other expenses are within the official federal government travel per diem rate for Palo Alto, CA.

22. Describe the type and class of transportation being provided. Indicate whether coach, business-class or first class transportation will be provided. If first-class fare is being provided, please explain why first-class travel is necessary:

Stanford University's Hoover Institution will provide coach-class round-trip airfare between D.C and San Fransisco, and round-trip ground transportation between Stanford University from SFO airport.

23. ☒ I represent that the travel expenses that will be paid for or reimbursed to Senate invitees do not include expenditures for recreational activities, alcohol, or entertainment (other than entertainment provided to all attendees as an integral part of the event, as permissible under Senate Rule 35).

24. List any entertainment that will be provided to, paid for, or reimbursed to Senate invitees and explain why the entertainment is an integral part of the event:

None

25. I hereby *certify* that the information contained herein is true, complete and correct. (You must include the completed signature block below for each travel sponsor.):

Signature of Travel Sponsor: Michael G. Franc

Name and Title: Michael G. Franc, Director of Washington, DC Programs

Name of Organization: Hoover Institution

Address: 1399 New York Ave NW, Suite 500, Washington, DC 20005

Telephone Number: (202) 760-3200

Fax Number: (202) 760-3191

E-mail Address: mfranc@stanford.edu

0000000057995

HART SENATE OFFICE BUILDING, ROOM 220
SECOND AND CONSTITUTION AVENUE, NE
WASHINGTON, DC 20510-6425

TELEPHONE: (202) 224-2981
FACSIMILE: (202) 224-7416
TDD: (202) 228-3752

United States Senate

SELECT COMMITTEE ON ETHICS

August 2, 2017

Michael K. Stransky
Republican Policy Committee
United States Senate
Washington, DC 20510

Dear Mr. Stransky:

This responds to your recent correspondence concerning an invitation you received to travel to the 2017 Stanford Congressional Cyber Boot Camp, in Palo Alto, California on August 14-17, 2017, sponsored by Stanford University's Hoover Institution (Hoover Institution). The Hoover Institution certified to the Select Committee on Ethics (the Committee) that it will pay the *necessary expenses*[1] related to the travel and that it is neither a lobbyist, nor lobbying firm, nor agent of a foreign principal, and it is not otherwise acting as a representative or agent of a foreign government. However, the Hoover Institution has certified that it is an organization designated under § 501(c)(3) of the Internal Revenue Code[2] that retains or employs a registered lobbyist and that no registered lobbyist will accompany you at *any point throughout your trip*.[3]

Based on information and materials available to the Committee, and assuming the **actual** travel and travel-related expenses conform to the information and materials you provided, it appears that the proposed payment or reimbursement of necessary expenses for this trip **may be accepted** under relevant Senate Rules and the Committee's *Regulations and Guidelines for Privately-Sponsored Travel*, so long as at the time of the payment or reimbursement, Hoover Institution is neither a registered lobbyist nor lobbying firm under the Lobbying Disclosure Act of 1995, nor an agent of a foreign principal under the Foreign Agents Registration Act (and is not otherwise acting as a representative or agent of a foreign government), and provided the travel and all required documents are disclosed to the Secretary of the Senate in accordance with the provisions of Senate Rules 34 and 35.

Under Senate Rule 35, Senate staff must receive advance authorization signed by the Member or officer under whose direct supervision the individual works in order to accept payment or reimbursement for necessary expenses related to fact-finding travel. Further, such authorization and expenses must be disclosed to the Secretary of the Senate by filing the

---

[1] The term "necessary expenses" has a specific definition. *See Select Committee on Ethics' Regulations and Guidelines for Privately-Sponsored Travel – Glossary of Terms* at 8.

[2] 26 U.S.C. § 501(c)(3).

[3] The term "any point throughout your trip" has a specific definition. *See Select Committee on Ethics' Regulations and Guidelines for Privately-Sponsored Travel – Glossary of Terms* at 2.

completed *Employee Pre-Travel Authorization* and the *Employee Post-Travel Disclosure of Travel Expenses* (Form RE-1 and Form RE-2), along with a copy of the *Private Sponsor Travel Certification Form,* and all relevant attachments (e.g., the private sponsor's invitation and itinerary) **within 30 days of the conclusion of Privately-Sponsored Travel**.

Finally, Senate Rule 34 requires a reporting individual,[4] on his or her Financial Disclosure Report, to make an annual disclosure of the receipt of payments or reimbursements under Senate Rule 35 from a private sponsor for officially-related travel expenses where, in the aggregate, travel expenses exceed $390 from that sponsor during a calendar year. However, if a Member, officer, or employee properly reports the receipt of necessary expenses for such travel to the Secretary of the Senate within 30 days of the travel, as discussed above, the travel expenses need not be disclosed a second time on their Financial Disclosure Report.

I hope you find this information helpful. If you have any additional questions, please do not hesitate to contact the Committee.

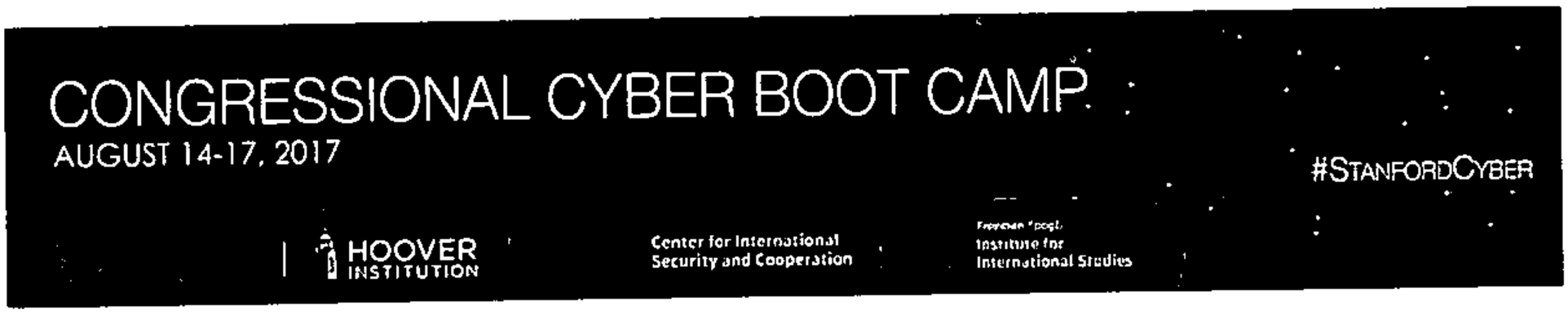
Sincerely,

Deborah Sue Mayer

Deborah Sue Mayer
Chief Counsel and Staff Director

Enclosure: Travel Checklist

[4] A reporting individual is someone whose salary equals or exceeds 120% of the basic rate of pay for GS-15 ($124,406 for CY 2017) or is a political fund designee and is required to file Financial Disclosure Reports.



SYLLABUS

FACULTY CO-CHAIRS

Dr. Amy Zegart
Co-Director, Center for International Security and Cooperation (CISAC)
Davies Family Senior Fellow, Hoover Institution
Senior Fellow, Freeman Spogli Institute for International Studies (FSI)
Professor of Political Science (by courtesy), Stanford University

Dr. Herb Lin
Senior Research Scholar for Cyber Policy and Security, Center for International Security and Cooperation (CISAC)
Hank J. Holland Fellow in Cyber Policy and Security, Hoover Institution
Chief Scientist Emeritus, Computer Science and Telecommunications Board, National Academies

COURSE DESCRIPTION

Modern nations are increasingly dependent on information and information technology for societal functions. Thus, ensuring the security of information and information technology — cybersecurity — against a broad spectrum of hackers, criminals, terrorists, and state actors is a critical task for the nation. Cybersecurity challenges are evolving at a rapid pace, and the cyber threat the nation faces today will be different from the one it faces tomorrow.

Cybersecurity is not solely a technical matter, although it is easy for policy analysts and others to get lost in the technical details. Improving cybersecurity is a multi-faceted enterprise that requires drawing on knowledge from computer science, economics, law, political science, psychology, and a host of other disciplines. Therefore, this Boot Camp draws upon the expertise of cyber scholars in academia as well as senior business and security professionals in Silicon Valley to provide perspectives on the many dimensions of this dynamic issue.

This Boot Camp will integrate multiple perspectives and disciplines to provide an understanding of the fundamentals of cybersecurity, the nature of cybersecurity threats, various approaches to

addressing these threats, and the use of offensive cyber capabilities to advance national interests. The Stanford Cyber Boot Camp endeavors to give congressional staffers a conceptual framework to understand the threat environment of today and how it might evolve so that they are better able to anticipate and manage the problems of tomorrow.

Day 1 (Monday, August 14): Cyber Attacks and Responses

12:00 p.m. – 1:00 p.m.: Lunch & Keynote Address

FRAMING THE CYBERSECURITY PROBLEM

Faculty:

Sean Kanuck, *Former National Intelligence Officer for Cyber Issues, Office of the Director of National Intelligence; CISAC affiliate*

This session will overview the scope of the program (what we cover, what we don't, and why) and set the analytic stage for how we approach the rest of the course.

Scope: The security implications and challenges of the nation's use of information technology. The course does not address topics such as consumer security, although many concepts covered are relevant.

Framing Theme #1: Cybersecurity has different meanings and poses different challenges to different stakeholders. Approaching the problem posed requires understanding the perspectives of various actors, their interests, incentives, and organizational demands. Boot Camp sessions are designed to allow staffers to better understand the perspectives of different stakeholders and key players, including attackers and corporate executives.

Framing Theme #2: The non-technical dimensions of cybersecurity (politics, organizational dynamics, economics, and psychology) are often far more important and less understood than the technical aspects. The Boot Camp pays explicit attention to these non-technical dimensions and how they intersect with technical challenges.

Framing Theme #3: On the technical side, the course focuses on the underlying foundational principles of computing and communications technology (collectively, information technology) that drive the evolution of architectures, technologies, and vulnerabilities.

Framing Theme #4: The Boot Camp explains the inherent dominance of offense over defense in cybersecurity and how this fact relates to the "cybersecurity problem."

1:00 p.m. – 2:00 p.m.: Session 1

THINKING LIKE AN ATTACKER

Faculty:

Peiter Zatko, *Cyber Independent Testing Lab*
Dr. Herb Lin (Discussant), *Senior Research Scholar, CISAC; Hank J. Holland Fellow, Hoover Institution*

Effectively combating any adversary requires understanding the ways in which that adversary thinks. Cybersecurity adversaries — from state agents seeking to disable military systems to hacktivists seeking to make a political point — share a security mindset: a predilection for examining the ways in which the security of a system can be circumvented or penetrated. Whereas good engineering is about how a system can be made to work, the security mindset involves thinking about how some aspect of a system can be made to fail. Understanding this mindset is the first step towards designing sound cybersecurity solutions.

Assignment: While in transit to the course location in Palo Alto, conduct a thought experiment for bringing an item prohibited by TSA regulations onto the airplane.

Learning Objectives: Why defense is more difficult than offense and what makes ongoing offense-defense competition inevitable.

2:30 p.m. – 3:30 p.m.: Session 2

THREATS TO CYBERSECURITY

Faculty:

Carey Nachenberg, *Google X; Adjunct Assistant Professor of Computer Science, UCLA*

Cybersecurity compromises can take a variety of forms and occur for a variety of reasons. Session 2 examines these compromises and the vulnerabilities in information technology that allow them to happen, again reprising the theme of offensive dominance. This session will include a number of forensic case studies that illuminate the attack spectrum, key challenges, and trends.

Learning Objectives: Security-relevant principles of information technology; types of compromise; the inherent vulnerabilities of information technology; the hidden complexity of cyberspace; anatomy of security compromises; and the spectrum of threats to cybersecurity.

3:45 p.m. – 4:15 p.m.: Keynote Remarks

THE VIEW FROM EUROPE

Faculty:

Toomas Hendrik Ilves, *Former President of Estonia; Distinguished Visiting Fellow at CISAC, Hoover, and FSI*

4:30 p.m. – 5:30 p.m.: Dinner & Session 3

OFFENSIVE DIMENSIONS OF CYBERSECURITY

Faculty:

Jason Healey, *Senior Research Scholar, Columbia University's School for International and Public Affairs*
Dr. Herb Lin, *Senior Research Scholar, CISAC; Hank J. Holland Fellow, Hoover Institution*

Offensive activities — including those conducted for espionage and attack purposes —serve a variety of national goals. These goals include, but are not limited to, cyber defense. This discussion will summarize the required strategy, intelligence, and policy necessary for offensive cybersecurity.

Learning Objectives: The role of offensive operations in cyberspace for improving the nation's cybersecurity posture and for other purposes; the differences between attacks and exploitations and the importance of these differences; the scope and nature of U.S. command and control of offensive operations in cyberspace.

6:00 p.m. – 8:30 p.m.: Session 4

SIMULATION: RESPONDING TO A CYBER CRISIS

Faculty:

Michael McNerney, *Cofounder and CEO of Efflux Systems; CISAC Affiliate*
Raj Shah, *Managing Partner, Defense Innovation Unit Experimental (DIUx)*
Joe Sullivan, *Chief Security Officer, Uber*
Ruby Zefo, *Vice President of the Law & Policy Group and Chief Privacy & Security Counsel, Intel Corporation*
Dr. Amy Zegart, *Co-Director, CISAC; Davies Family Senior Fellow, Hoover Institution; Senior Fellow, FSI*

In this exercise, congressional staffers assume the roles of business executives at a large tech company called Frizzle that has just discovered a major cyber breach. Early forensics indicate that a Frizzle employee opened a malicious PDF file containing a zero-day exploit. This vulnerability enabled the attackers to gain access to F-Net, the company's social networking platform, as well as the Frizzle email user accounts of Chechen activists and sympathizers. In addition, the malicious file may have spread through victims' emails to the Credit Luxe bank in Luxembourg, which processes more than two thirds of Frizzle's user payments. Frizzle's engineering/cybersecurity team, which is one of the best in the world, believes the attack came from Eastern Europe, though much remains unclear.

The CEO has called an emergency meeting of the Board of Directors to formulate a broad-based response to the cyber breach and has asked each of Frizzle's core teams – Engineering / Cybersecurity, Business Strategy, Legal, Public Policy, and Marketing / Communications – to develop and present actionable recommendations to the Board.

The Board of Directors is played by leading Silicon Valley security specialists, lawyers, and entrepreneurs with extensive experience in cybersecurity and business. Board Members attend team breakout sessions and in the "full board meeting" question and discuss each team's recommendations. The simulation concludes with a debrief session where staffers reflect on the simulation and Board Members share insights from their actual experiences confronting cyber challenges.

Learning Objectives: To walk in the shoes of business leaders confronting the early hours and critical decisions of a cyber crisis. Who exactly is hurt or could be hurt by the breach? How could the breach impact Frizzle's business in different markets and its brand reputation? Who are the key stakeholders and how might they react? What actions should Frizzle take and what are the tradeoffs? Should the company "hack back" or publicize the breach to its users, its European bank, its competitors? Work with U.S. government agencies? How do Frizzle's mission and corporate culture guide its response? These are some of the questions staffers will consider.

Day 2 (Tuesday, August 15): Deep Dive: Technical & Nontechnical Aspects of Cyber

8:30 a.m. – 10:00 a.m.: Breakfast and Keynote Conversation

KEYNOTE **Conversation with Dr. Condoleezza Rice and Marc Andreessen**

Faculty:

Dr. Condoleezza Rice, *Thomas and Barbara Stephenson Senior Fellow, Hoover Institution; Denning Professor, Stanford Graduate School of Business; former U.S. Secretary of State and National Security Advisor*

Marc Andreessen, *Cofounder and General Partner of Andreessen Horowitz*

10:15 a.m. – 11:15 a.m.: Session 5

FUNDAMENTAL PRINCIPLES OF CYBERSECURITY

Faculty:

Dr. Irving Lachow, Portfolio Manager, International Cyber, MITRE; *Visiting Fellow, Hoover Institution; Affiliate, CISAC*

Dr. John Villasenor, *Professor of Electrical Engineering, Public Affairs, and Management, UCLA; Vice Chair, World Economic Forum's Global Agenda Council on the Intellectual Property System; Visiting Fellow, Hoover Institution; Affiliate, CISAC*

Although cybersecurity can be a deeply technical subject, especially in how cybersecurity solutions are implemented, a few fundamental principles underlie most solutions. This session takes a deep dive into the fundamental principles of improving cybersecurity and how they fit together. These include reducing reliance on information technology, detecting cybersecurity compromises, and blocking and limiting the impact of compromise. Additional topics include authentication, access control, forensics, recovery, containment, resilience, and active defense.

Learning Objectives: The value of these fundamental principles of cybersecurity and how they can be used collectively to improve security.

11:45 a.m. – 12:45 p.m.: Lunch & Session 6

ECONOMIC, PSYCHOLOGICAL & ORGANIZATIONAL DIMENSIONS OF CYBERSECURITY

Faculty:

Dr. Dave Clark, *Senior Research Scientist at the MIT Computer Science and Artificial Intelligence Laboratory*

Dr. Tyler Moore, *Tandy Assistant Professor of Cyber Security and Information Assurance, University of Tulsa*

Known cybersecurity measures are often fully adopted due to a variety of economic, psychological, and organizational factors. These factors are non-technical in nature and often underappreciated by technical and policy communities. Economics describe the incentives that apply to cyber defenders and adversaries, including the nature of cybersecurity market failures and the ability to handle collective action problems. Psychology addresses the deception primary to cybersecurity attacks and the uncertainty of most decision-making in response. An organizational perspective addresses the structural necessities and importance of organizational culture to cybersecurity. This session examines how these factors often discourage the adoption of sound security practices.

Learning Objectives: The importance of economic, organizational, and psychological factors of cybersecurity and why they are often overlooked in efforts to improve cybersecurity; how government action might help to address non-technical factors that diminish the nation's cybersecurity posture.

1:30 p.m. – 2:30 p.m.: Session 7

DOMESTIC LAW AND INTERNATIONAL LEGAL DIMENSIONS OF CYBER SECURITY

Faculty:

Prof. Matthew Waxman, *Liviu Librescu Professor of Law, Faculty Chair Roger Hertog Program on Law and National Security, Columbia University*

Prof. Robert Chesney, *Associate Dean and Charles I. Francis Professor, University of Texas School of Law; Director, Robert S. Strauss Center for International Security and Law*

Technological change has far outpaced changes in law and will almost certainly continue to do so in the future. This lag consequentially challenges Congress to craft legislation appropriate for future technology. Furthermore,.nations have cooperative and competitive (and sometimes

adversarial) interests that play out in cyberspace. Internet communication does not inherently respect national borders, giving an international dimension to every cybersecurity challenge.

Learning Objectives: For domestic law, the implicit technological assumptions of existing cybersecurity laws; what problems arise in applying existing law to technological circumstances not contemplated at the time of initial passage.

For international dimensions, various legal regimes of potential relevance, including the law of war, human rights law, trade and intellectual property law; proposals for Internet governance; and different non-governmental organizations that affect the design and operation of the Internet.

2:30 p.m. – 3:00 p.m.

DEBRIEF from previous day

Faculty:

Dr. Herb Lin, *Senior Research Scholar, CISAC; Hank J. Holland Fellow, Hoover Institution*
Dr. Amy Zegart, *Co-Director, CISAC; Davies Family Senior Fellow, Hoover Institution; Senior Fellow, FSI*

5:30 p.m. – 8:30 p.m.: Reception & Dinner

KEYNOTE **Conversation between Dr. Michael McFaul and Joel Peterson**

Faculty:

Dr. Michael McFaul, *Director and Senior Fellow, FSI; Peter and Helen Bing Senior Fellow, Hoover Institution, Professor of Political Science, Stanford University; former U.S. Ambassador to the Russian Federation*
Joel Peterson, *Chairman, Jet Blue Airways; Robert L. Joss Adjunct Professor of Management, Stanford Graduate School of Business; Chairman, Hoover Institution Board of Overseers*

Day 3 (Wednesday, August 16): Civil Liberties, Corporate Interests, and Security

7:45 a.m. – 8:30 a.m.: Breakfast

DEBRIEF from previous day

Faculty:

Dr. Herb Lin, *Senior Research Scholar, CISAC; Hank J. Holland Fellow, Hoover Institution*
Dr. Amy Zegart, *Co-Director, CISAC; Davies Family Senior Fellow, Hoover Institution; Senior Fellow, FSI*

8:30 a.m. – 9:30 a.m.: Session 8

CYBERSECURITY AND CIVIL LIBERTIES

Faculty:

Anne Neuberger, *National Security Agency*
Jennifer Granick, *Director of Civil Liberties, Stanford Center for Internet and Society; Affiliate, CISAC; Former Civil Liberties Director, Electronic Frontier Foundation*

Measures intended to support cybersecurity can also threaten certain civil liberties. What cybersecurity means depends in part on whose security is at risk. For some, a threat to civil liberties resulting from greater use of information technology might be interpreted as a cybersecurity threat. Session 8 focuses on this push and pull between security and civil liberties in cyberspace.

Learning Objectives: Different perspectives at the nexus of civil liberties and cybersecurity; how, when, and to what extent, preservation of civil liberties and cybersecurity trade off against one another. Topics to be discussed include privacy, anonymity, and free speech.

9:30 a.m. – 10:30 a.m.: Session 9

CORPORATE PERSPECTIVES ON CYBERSECURITY

Faculty:

Dr. Sameer Bhalotra (Chair), *Co-Founder and CEO, StackRox; Senior Associate of the Strategic Technologies Program, CSIS; Affiliate, CISAC; former Senior Director for Cybersecurity, National Security Council*
Rick Howard, *Chief Security Officer at Palo Alto Networks*
Matt Miller, *Partner at Sequoia Capital*

Market forces have a critical role in enhancing or weakening cybersecurity. Session 9 examines how such forces play out at the level of the individual firm and incorporate the views and concerns of the business community. Silicon Valley senior executives and engineers will give their "cyber-ground truths" about the security problems facing the private sector.

Learning Objectives: Various private sector perspectives from technology firms that support innovative efforts for providing IT-based products and services with attention to cybersecurity.

11:00 p.m. – 11:45 p.m.: Session 10

WHITE HOUSE PERSPECTIVES

Faculty:

Andy Grotto, *CISAC Perry Fellow; Hoover Research Fellow; Affiliate, CISAC; Former Senior Director for Cybersecurity Policy, National Security Council*

12:00 p.m. – 1:30 p.m.: Lunch Keynote

DRIVERLESS CARS & PLANE HACKING: SECURITY VULNERABLITIES, CAUSES, AND CHALLENGES

Faculty:

Dr. Stefan Savage, *Professor of Computer Science and Engineering, UCSD; Director, Center for Network Systems (CNS); Co-Director, Center for Evidence-based Security Research (CESR)*

Modern automobiles are no longer mere mechanical devices; they are pervasively monitored and controlled by dozens of digital computers coordinated via internal vehicular networks. While this transformation has driven major advancements in efficiency and safety, it has also introduced

a range of new potential risks. In 2010, University of California, San Diego and the University of Washington demonstrated the ability to remotely control a popular passenger vehicle with no prior physical access. Recent demonstrations have validated that similar issues exist in other vehicles as well.

Learning Objectives: The nature of automotive security vulnerabilities, the underlying causes, and the challenges (both technical and non-technical) in securing the automotive platform.

2:30 p.m. – 4:30 p.m.

TESLA FACTORY VISIT

45500 Fremont Blvd, Fremont, CA 94538

5:30 p.m. – 8:30 p.m.

DINNER & FEEDBACK SESSION

Coupa Café – Stanford Golf Course
198 Junipero Serra Blvd, Stanford, CA, 94305